Scientific Research Publishing

Int. J. Communications, Network and System Sciences, 2017, 10, 75-105
http://www.scirp.org/journal/ijcns
ISSN Online: 1913-3723
ISSN Print: 1913-3715

A Systems-Theoretic Security Model for Large Scale, Complex Systems Applied to the US Air Transportation System

Joseph R. Laracy

Department of Mathematics and Computer Science, Seton Hall University, South Orange, NJ, USA
Email: joseph.laracy@shu.edu

How to cite this paper: Laracy, J.R. (2017) A Systems-Theoretic Security Model for Large Scale, Complex Systems Applied to the US Air Transportation System. *Int. J. Communications, Network and System Sciences*, **10**, 75-105.
https://doi.org/10.4236/ijcns.2017.105005

Received: April 23, 2017
Accepted: May 28, 2017
Published: May 31, 2017

Abstract

Classical risk-based or game-theoretic security models rely on assumptions from reliability theory and rational expectations economics that are not applicable to security threats. Additionally, these models suffer from serious deficiencies when they are applied to software-intensive, socio-technical systems. A new approach is proposed in this paper that applies principles from control theory to enforce constraints on security threats thereby extending techniques used in system safety engineering. It is applied to identify and mitigate the threats that could emerge in critical infrastructures such as the air transportation system. Insights are provided to assist systems engineers and policy makers in securely transitioning to the Next Generation Air Transportation System (NGATS).

Keywords

Air Transportation, Security, Systems Engineering, Control Theory, System Dynamics

1. Introduction

The increasing complexity and interconnectedness of large scale systems have introduced new vulnerabilities to those infrastructures. Large scale, complex systems require physical, communication, computer, information, and operational security. Vulnerabilities often emerge in an engineering system when one or more of the aforementioned aspects are omitted. Attackers rarely choose to directly engage the most secure aspects of a system, such as the cryptographic algorithms. The interdisciplinary nature of the security problem is one of the key factors that make the solution so elusive. Traditional, disciplinary approaches, on their own, are often insufficient to accomplish the security goals of a complex

system. Only a comprehensive methodology has the potential to succeed [1].

2. Next Generation Air Transportation System (NGATS)

In 2004, the US Congress passed the Vision 100—Century of Aviation Reauthorization Act in response to pressures on the current US air transportation system (ATS). Post 9/11 economics and demand asymptotically approaching capacity at many key airports necessitated a radically new approach. A senior policy team made up of the Secretary of Transportation (Chair), Secretary of Defense, Secretary of Homeland Security, Secretary of Commerce, Director of the Office of Science and Technology Policy, Administrator of the National Aeronautics and Space Administration (NASA), and Administrator of the Federal Aviation Administration (FAA) was formed to provide policy guidance. Also, a Joint Program Development Office (JPDO) was created to manage the development of the Next Generation Air Transportation System (NGATS).

The United States ATS faces challenges in three areas: security, gridlock, and maintaining global leadership. In light of these realities, the customs service has been forced to substantially modify its procedures to accommodate a major increase in international passenger and cargo volume. Gridlock is already a major problem at US metropolitan airports and one hour wait times are often encountered by millions of Americans. Preliminary economic models predict that the cost due to congestion for US consumers could easily reach into the billions. If the congestion issue is not resolved, same-day travel and reliable scheduled travel will exist only in people's memories.

The variety of transportation options is also expected to increase in the coming decades. UAVs, micro-jets (5 passengers), super jumbo-jets (600 passengers +), and other 21st century innovations may radically change US airspace. Small perturbations in how people travel and transport goods will require major overhauls of the transportation infrastructure. According to the JPDO, "a shift of 2% of today's commercial passenger to micro-jets that seat 4 - 6 passengers would result in triple the number of flights in order to carry the same number of passengers" [2].

The JPDO has three performance goals [2]:

1. Satisfy future growth in demand (up to three times current levels) and operational diversity
2. Reduce transit time and increase predictability (domestic curb-to-curb transit time cut by 30%)
3. Minimize the impact of weather and other disruptions (95% on time)

However, the uncertainty associated with the profile of aircraft in the coming decades makes it difficult to develop a strategy. Parallel runways, improved wake vortex sensing, and relaxation of single runway occupancy restrictions are being considered to improve system throughput. Without expensive ground-based equipment, the JPDO hopes to have precision approaches available on every US runway.

Aircraft themselves will need to operate with greater autonomy to achieve the

goals of NGATS. In some cases, co-pilots will be replaced by computers; in others, there will be no pilot at all. UAVs will be subject to reduced separation standards, and more flexible spacing will be applied to both aircraft in-flight and on the ground. Additionally, a paradigmatic shift is planned for air traffic control (ATC). Controllers will move from controlling individual aircraft to managing airspace based on flows. There exists a large body of knowledge around optimization of network flows that will surely guide these efforts. For example, much work has been done at the Draper Laboratory that offers powerful techniques for UAV route planning, e.g. [3]. Other changes include the elimination of voice communication (under normal conditions) from data link capable aircraft, and the incorporation of new technologies that make two sets of flight procedures (instrument and visual) unnecessary.

Given the proposed changes, the pressing question remains: "How can the US transition to NGATS in such a way that security improves, rather than worsens?" With the goal of assisting JPDO leaders in making an informed decision, this research provides a systematic review of the threats that could emerge. Also, acknowledging the colossal failure of the FAA's Advanced Automation System in the mid-1990s resulting in $2.9 billion spent on a system that was never deployed [4], the JPDO must not allow complexity to grow out of control. The author's hypothesis is that the new method, outlined later in this paper, provides valuable insights into such security problems.

3. Traditional Techniques

3.1. Classical Approaches

A variety of approaches exist both in industrial practice and the academic literature for conducting security analyses on large infrastructure systems. These methods include "best practice engineering", quantitative risk assessment, game theory, and red teaming. The four classical approaches each have their own strengths and weaknesses, but unfortunately do not provide total coverage for the system security problem.

The most common security technique is simply to apply best practices. This approach is usually conducted in an unsystematic way and reduces or removes only the most obvious vulnerabilities [5]. If a systematic approach is taken to develop a comprehensive body of best practice literature, the best practice approach would be far more useful to engineers developing large systems. Usually, security engineers will employ one or more of the following methods to supplement best practice approaches.

3.2. Risk Analysis

Risk-based security seeks to quantify security risks by assigning severity and likelihood ratings to attack scenarios. The emphasis of this technique has been on risk-based decision-making whose goal is to direct security investments as opposed to modeling particular kinds of threats. The approach is derived from reliability models of accident causation that are rooted in a chain-of-events pers-

pective. Whether part of a preliminary hazard analysis or an accident reconstruction activity, the reliability engineer attempts to understand the potential or actual accident by identifying the events or faults that could initiate the accident. Such fault and event trees are usually part of a method called probabilistic risk assessment (PRA). The goals of PRA are to estimate both the likelihood and severity of a risk. PRA was developed in the mid-1970s to improve nuclear power plant safety. Professor Norm Rasmussen of MIT chaired the Reactor Safety Study that was the first real probabilistic risk assessment [6].

A probabilistic risk assessment is a four step process:

1. Identify undesirable events.
2. Identify accident scenarios (sequences of events).
3. Estimate the probability of each scenario either based on statistical testing data, or expert judgment if scenarios are rare.
4. Rank the accident scenarios according to likelihood.

The framework yields a probability for each undesirable event identified in the first stage.

PRA turned out to be very successful for assessing risks in nuclear power shut-down systems. Such systems were historically very simple, electro-mechanical systems designed to minimize unnecessary complexity, and used proven analog electrical technologies. PRA carries with it a number of important assumptions:

1. The events or faults at each node in the trees are collectively exhaustive—all possible events are identified.
2. The events or faults at each node in the trees are mutually exclusive—they cannot occur simultaneously.
3. The probability of each scenario is accurate enough to be useful to decision makers.

In a reactor shut-down system, nuclear engineers with decades of experience can probably develop trees that satisfy the first two assumptions due to their intimate knowledge of reactor design and operation. Furthermore, component technologies such as electrical relays could be extensively tested in the laboratory to compute reliability metrics such as mean time between failures (MTBF).

However, when complex systems like the Space Shuttle are considered, serious questions arise regarding the appropriateness of PRA. For instance, how does software change the picture? How can the MTBF of unique digital electronics be estimated? How many events or faults must be accounted for? Herein lies the problem of applying PRA to software-intensive systems [7]. Software does not wear out and fail; it only implements a set of requirements that may or may not be correct. In practice, PRA analysts utilize subjective probability (expert judgment) when thousands of laboratory MTBF tests cannot be carried out. However, software in one environment may produce desirable behavior, while in a slightly different one it may lead to disaster. Therefore, the meaning of the subjective probability value is not clear. Additionally, if a spacecraft computer has 128 MB of memory, or 2^{30} bits, then it has $2^{\text{number of bits}}$ or $2^{2^{30}}$ states. Clearly,

each state cannot be analyzed.

Before the Space Shuttle Challenger disaster, NASA headquarters reported the probability of a failure with loss of vehicle and human life as 10^{-5} [8]. Before the Space Shuttle Columbia disaster, the reported probability was 1/250 [9]. According to NASA space operations spokesman, Allard Beutel, the revised *post*-Columbia figure became 1/100 [10]. Recently, researchers in the field of PRA acknowledged that PRA should not be the sole basis for decision making and that the quantitative results should be part of risk-informed, not risk-based decisions. They acknowledge that human factors, software, safety culture, and design errors are not well handled by PRA [11].

Given the central role of human factors, software, culture, and design errors in security, PRA's applicability to security problems is also dubious. Donn Parker makes an insightful observation in this regard [12]:

> Security risk is not measurable, because the frequencies and impacts of future incidents are mutually dependent variables with unknown mutual dependency under control of unknown and often irrational enemies with unknown skills, knowledge, resources, authority, motives, and objectives—operating from unknown locations at unknown future times with the possible intent of attacking known but untreated vulnerabilities that are known to the attackers but unknown to the defenders.

See [13] for a review of the work of a variety of researchers who have attempted to supplement pure, reliability-based PRA with other techniques to make it relevant to security.

3.3. Game Theory

Bier [14] asserts that managing risks from intelligent adversaries is very different from other types of risk and suggests game theory over decision theory. Previous work in this area focused on "policy insights" such as the relative merits of deterrence and other protective measures [15]. Sandler and Arce [16] present a number of compelling reasons for the applicability of game theory to security problems:

1. Game theory captures the strategic interactions between terrorists and a targeted government, where actions are interdependent and, thus, cannot be analyzed as though one side is passive.
2. Strategic interactions among rational actors, who are trying to act according to how they think their counterparts will act and react, characterize the interface among terrorists or among alternative targets.
3. In terrorist situations, each side issues threats and promises to gain a strategic advantage.
4. Terrorists and governments abide by the underlying rationality assumption of game theory, where a player maximizes a goal subject to constraints.
5. Game-theoretic notions of bargaining are applicable to hostage negotiations and terrorist campaign negotiations over demands.

6. Uncertainty and learning in a strategic environment are relevant to all aspects of terrorism, in which the terrorists or government or both are not completely informed.

However, game theory requires strong assumptions about the availability of mutual information and the rationality of opponents [17]. As mentioned earlier, empirical work by Tversky and Kahneman [18] has shown that these assumptions often break down in reality. Additionally, traditional games are organized to pursue a minimax solution for a two-person, zero-sum game. However, as Banks and Anderson point out, such a model is only an approximation because defender and attacker will value successful and failed attacks differently [17].

Many game-theory models of security carry the traditional, simplifying assumption that the probability of a successful terrorist attack on a location is a convex function of the defensive resources. Some security measures, such as relocating a facility to a more secure location, are inherently discrete. Discretization introduces step changes into the function so there is no longer a smooth, convex function due to declining marginal returns on defensive investments. Also, if a particular level of defensive investment completely deters an attack, the probability of terrorist success drops rapidly beyond that point. This scenario would also produce a non-convex function in certain regions. When non-convex functions are permitted, multiple local optima may emerge, thereby complicating the defense resource allocation problem [17]. In order to populate payoff matrices with values, statistical techniques from quantitative risk assessment are usually used [20].

According to Fricker [19], game theory's role in security focuses on analyses related to:

1. Assessing strategies for how national antiterrorism expenditures,
2. Measuring how military strategies encourage/discourage terrorism,
3. Assessing insurance risks,
4. Evaluating the effects of focusing either on deterrence or preemption.

As the list above indicates, game-theoretic models focus on strategic decision making. They do not directly support the design and operation of infrastructure systems that may be the target of terrorist attacks.

3.4. Red Teams

Red teaming is an excellent activity to complement other security analyses as well as reduce the complacency that often sets in after extended periods without attacks. The goal of any red team is to challenge the plans, programs, and assumptions of the client organization. Teams may challenge organizations at strategic, operational, or tactical levels depending on the area that needs the most attention. The words of William Schneider, Jr., Chairman of the Defense Science Board, best capture the state of red teaming: "Red teams can be a powerful tool to understand risks and increase options. However, the record of use of red teams in DoD is mixed at best" [20].

The greatest benefit derived from red teaming exercises is "hedging against

catastrophic surprises". A good red team is capable of elucidating a deeper understanding of an adversary's options, and identifying vulnerabilities in concepts, programs, plans, postures, and strategies. Red teams also challenge "the accepted assumptions and accepted solutions" as well as identify inexperience. They may function as surrogate adversaries, devil's advocates, or simply as sources of independent judgment.

Schneider also points out that "red teaming is important but it is not easy nor often done very well". He identifies the following causes of failure [20]:

The red team:

1. Does not take its assignment seriously.
2. Could lose its independence.
3. Could be too removed from the decision making process.
4. Could have inadequate interaction with the "blue" (team) and be viewed as just another sideline critic.
5. Could destroy the integrity of the process and lose the confidence of decision makers by leaking its findings to outsiders.

Red team effectiveness is easily impaired by a corporate culture that does not value criticism and challenge, managers that do not want issues to arise that may "rock the boat", dysfunctional interaction between red and blue teams, unqualified red team staff, and calling in a red team when the problem has already grown out of control. The red team must have independence with accountability, as well as a process that enables the game results to be seriously considered by senior management [20]. Unfortunately, the red teaming process failed miserably before 9/11/2001. Testimony by Bogdan Dzakovic, a FAA Red Team veteran, to the National Commission on Terrorist Attacks upon the United States, on May 22, 2003, reveals how a good red team can become completely ineffective in the face of management resistance.

The Presidential Commission investigating the bombing of Pan Am 103 in 1990 created the FAA red teams that are in place today. After the TWA 800 crash, Congress passed the FAA Reauthorization Act of 1996. The law states that "…the Administrator [of FAA] shall conduct periodic and unannounced inspections of security systems of airports and air carriers to determine the effectiveness and vulnerabilities of such systems…" Later, in 1997, a White House Commission stated that "…Red Team testing should also be increased by the FAA, and incorporated as a regular part of airport security action plans. Frequent, sophisticated attempts by these Red Teams to find ways to dodge security measures are an important part of finding weaknesses in the system and anticipating what sophisticated adversaries of our nation might attempt" [21].

Unfortunately, as Dzakovic's testimony indicates, the value of these red teams has been seriously undercut [21]:

> Although we breached security with ridiculous ease up to 90% of the time, the FAA suppressed these warnings. Instead we were ordered not to retest airports where we found particularly egregious vulnerabilities to see if the problems had been fixed. Finally, the agency started providing advance no-

tification of when we would be conducting our "undercover" tests and what we would be checking.

For example, in the late 1990s, over two-thirds of red teams breached airport security with firearms undetected. This revelation led the FAA to stop testing with guns. According to Dzakovic, managers at the highest levels of the FAA chose to ignore warnings such as these: "What happened on 9 - 11 was not a failure of the system, it was a system designed for failure. FAA very consciously and deliberately orchestrated a dangerous façade of security". [21]

Compelling evidence existed prior to 9/11 of the likelihood and severity of this threat. In testimony to the US Senate Committee on Commerce, Science, and Transportation Subcommittee on Aviation Security on April 6, 2000, the Associate Administrator of the FAA for Civil Aviation Security stated: "Moreover, members of foreign terrorist groups and representatives from state sponsors of terrorism are present in the United States. There is evidence that a few foreign terrorist groups have well-established capability and infrastructures here" [21]. Additionally, many of the 9/11 hijackers were identified by the Computer Assisted Passenger Pre-Screening Systems (CAPPS). CAPPS is a system that automatically researches anyone that buys an airplane ticket and generates a risk score based on a variety of factors.

The following hijackers in **Table 1** were flagged by CAPPS [22].

Such a failure is not surprising when one learns that a FAA Security Special Agent wrote a letter to the Department of Transportation Inspect General in 1999 saying that "…Logan International Airport is in a critical state of non-compliance with Federal Aviation Security Regulations…" [22].

This paper presents a security model that does not rely on the assumptions of quantitative risk assessment, considers issues at a level closer to system design and operation compared to game theory, and supports successful red teaming.

4. Systems Theory and Complexity

4.1. Foundational Principles

Before explaining the systems-based methodology, it is important to understand its theoretical underpinning. In contrast to the traditional scientific method that relies on analytic reduction, systems theory states that complex systems must be considered holistically. The theory was well developed by Bertalanffy, Ashby,

Table 1. 9/11 terrorists identified by CAPPS.

Hijacked Aircraft	Terrorists
American Airlines Flight 11 (Logan)	Wail al-Shehri, Satam al-Suqami, Waleed al-Shehri, Mohamed Atta
American Airlines Flight 77 (Dulles)	Hani Hanjour, Khalid al-Mihdhar, Majed Moged, Nawaf al-Hazmi, Salem al-Hazmi
United Airlines Flight 93 (Newark)	Ahmad al-Haznawi
United Airlines Flight 175 (Logan)	None

and Wiener in the 1940s and 50s in response to challenges encountered in biology, communication, and control. During this time, scientists and engineers began to recognize a new type of complexity.

Organized simplicity is exhibited in traditional, deterministic systems that easily can be decomposed into subsystems and components such as in structural mechanics. The re-synthesis of the subsystems does not yield any unexpected properties because the component interactions are well defined and often linear. Conversely, it is not straightforward or useful to decompose systems that exhibit unorganized complexity. However, statistical techniques are applicable because of the regularity and randomness that characterize the network structure. The Law of Large Numbers becomes applicable and average values can be computed such as in statistical mechanics (e.g. ideal gases in chemistry). The "new" complexity theory, organized complexity, describes systems with a sufficiently complex structure to make it impractical or impossible for them to be modeled with analytic reduction, and not random enough to be modeled using statistics [23] see **Figure 1**.

Systems characterized by organized complexity exhibit strong, non-linear interactions and coupling between subsystems and components. Therefore, a top-down approach needs to be applied to such systems. Two underlying concepts provide insight into these complex systems: emergence & hierarchy and communication & control.

Abstractions for complex systems often involve layers. In the case where the abstraction is hierarchical, the level of organization increases as one moves toward higher layers. Additionally, the step from level n to $n + 1$ yields new properties that are not discernable at level n. This phenomenon is referred to as emergence, or emergent properties. For example, "The shape of an apple, although eventually explainable in terms of the cells of the apple, has no meaning

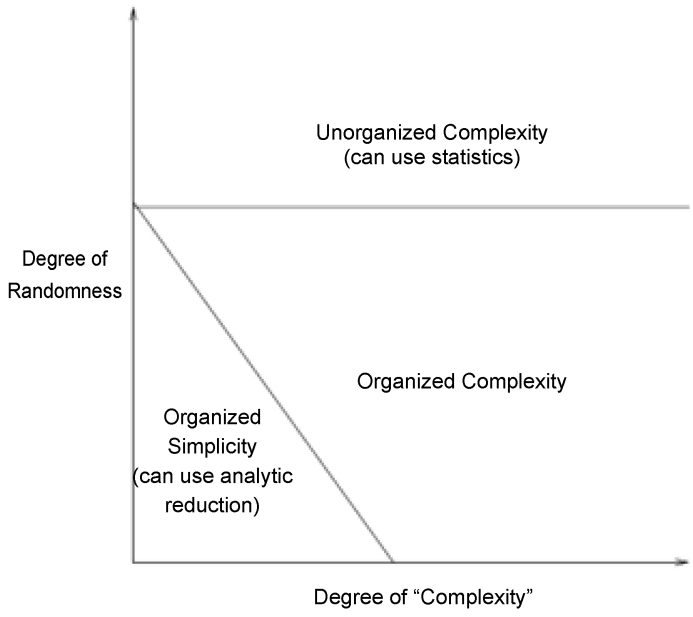

Figure 1. System organization and complexity. Image source [23].

at that lower level of description". [23] Security is an emergent system property. For example, it is not possible to completely evaluate the security of an individual personal computer in isolation.

The security of a PC can only be determined by its relationship within a broader context, *i.e.* a socio-technical system. A PC might be considered "secure" when it is sitting isolated at home. However, once that computer is brought to work, connected to the LAN, and therefore the Internet, a whole new class of vulnerabilities emerges. An individual computer may be bolted to a desk, require a boot-up password, and have an encrypted file system. However, a security expert would never classify such as system as "totally secure". This is because security is a *system* property. A computer network is more than the sum of individual PCs, the behavior of the PCs in isolation does not tell us all the possible behaviors it may exercise in connection with other computers, and the performance of a network cannot be characterized by a simple additive composition of PCs.

As Graham, Baliga, and Kumar point out, over the last 50 years, the fields of communications, control, and computation have converged [24]. The resulting theoretical foundations are contained in systems theory and directly relevant to the goals of system safety and security. One especially sees the need for communications to coordinate required control in open systems [23]. Control is exercised in complex systems by imposing constraints on lower levels in the hierarchy. According to Peter Checkland [25]:

> Control is always associated with the imposition of constraints, and an account of a control process necessarily requires our taking into account at least two hierarchical levels. At a given level, it is often possible to describe the level by writing dynamical equations, on the assumption that one particle is representative of the collection and that the forces at other levels do not interfere. But any description of a control process entails an upper layer imposing constraints upon the lower. The upper level is a source of an alternative description of the lower level in terms of specific function that are emergent as a result of the imposition of constraints.

Ashby provides four conditions that are required to exercise control over a system [26]:

1. Goal condition—The controller must have a goal or goals.
2. Action condition—The controller must be able to affect the state of the system.
3. Model condition—The controller must be (or contain) a model of the system.
4. Observability condition—The controller must be able to ascertain the state of the system.

The controller in Leveson's generic control loop (**Figure 2**) must be able to observe the controlled process through the sensors, relate the observation to its model, and actuate the process if the system has deviated from the goal condition.

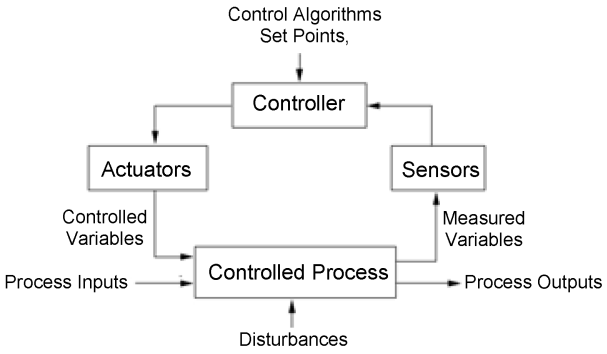

Figure 2. Generic control loop. Image source [26].

4.2. Systems Thinking

Systems thinking is the application of systems theory to mental models and thought. It acknowledges that learning is a feedback process and views problems through the lens of interconnected networks governed by systems of non-linear relationships. System thinkers advocate holism over the traditional reductionism found in modern science. Operations Researcher, Russell Ackoff, and Computer Engineer, Jay Forrester, developed the approach in the late 1950s in response to challenges encountered in studying complex, socio-technical systems. Forrester created the System Dynamics modeling technique, which is based on the theory of non-linear dynamics. His successors include Peter Senge, who applies systems thinking to organizational learning [27], and John Sterman, who uses it to improve managerial decision-making in complex systems [28].

Ackoff's system thinking is best understood as carrying on the spirit of Operations Research as it was practiced in the 1950s and 60s before mathematical methods overtook problem framing and formulation as the forte of OR specialists [29]. Ackoff's successor is Jamshid Gharajedaghi, the leader of the Interactive Design (ID) movement. ID focuses on human choice in socio-technical systems and incorporates iterative inquiry and operational thinking. Iterative inquiry theory suggests that to gain understanding in complex systems, a successive technique of investigating function, structure, process, and context can lead to greater understanding.

Operational thinking requires a system scientist to think about how systems actually work as opposed to how they could theoretically work. Non-operational thinking is best captured in econometric models that seek to predict milk consumption but do not factor in cows [30]. Overall, ID advocates participatory design and offers an approach both for formulating problems and developing solutions in teams [31].

In Britain, Peter Checkland developed another systems thinking approach for modeling organizational processes and managing change in complex social systems called the Soft Systems Methodology (SSM) [25]. SSM is a qualitative technique that seeks to impose systems thinking in non-systemic situations where human social activity is more important that other factors such as technology. Conceptual models and graphics are developed to promote deeper understand-

ing of the complex social system.

Systems thinking have yielded significant results in the Engineering Systems Division at MIT. In particular, it has proven to be very useful for the investigation of cultural and organizational factors that jeopardize the safety and security of complex engineering systems [32].

5. System Theoretic Accident Models and Processes for Security (STAMP-Sec)

5.1. Introduction to STAMP

STAMP-Sec views security incidents as the result of inadequate control, rather than strictly a failure, such as a cryptographic device breaking [33] or a cracked-code. Security is an emergent property that is achieved through the enforcement of constraints. This perspective allows security problems to be transformed into control problems for which powerful tools can be employed. Control structures are defined to capture the communication and control in the system and illustrate the presence or absence of feedback. They are hierarchal in nature and need to be constructed both for system development and system operation.

Security must be designed into a system as well as be part of how it is operated. Historical examples of large systems where security was added in "after the fact" have been plagued by systemic security risks. For example, current approaches to information security suffers from serious deficiencies as evidenced by the influence of SPAM, Internet worms, viruses, phishing, and other attacks that plague the common Internet user. This is largely a result of the fact that network research in the 1960s through the 1980s focused on achieving performance (e.g. throughput and robustness) objectives with little emphasis on security. As a result, when new threats began to emerge in the 1990s, Internet security was approached from an ad-hoc perspective—applying patches to vulnerabilities already identified by attackers. The problem remains that the underlying architecture was not designed to support strong security.

A STAMP control structure informs design by defining the necessary communication and control between subsystems and components to enforce security constraints. Effective communication between levels of the hierarchy is essential to successful system security. Layer $n + 1$ must be able to assert goals, policies, and constraints through a reference channel and layer n must be able to communicate operational experience through a measuring channel.

In a top-down security engineering activity, threat analyses may be conducted using a variant of STPA, (STAMP-based Analysis). Threats that the system must guard against are identified and constraints are defined that prevent their instantiation as a result of design or operational decisions. The complete list of constraints should be part of a system's requirements document. After that, the static control structure is modeled. Components in the control structure are assigned responsibility to maintain the constraints. Finally, possible control actions for the components are defined [34]. System Dynamics is used to understand how the control structure and the malicious actor could evolve.

The five steps of STAMP-Sec are provided below.

1. Identify the system level threats.
2. Write security constraints for the threats.
3. Define the static control structure to prevent or mitigate the threats.
   a. Assign constraints to the system components responsible for implementing them.
   b. Define the control actions for the components that prevent or mitigate the threats.
4. Identify inadequate control actions that could lead to an insecure state.
5. Determine ways that constraints could be violated and attempt to eliminate them. In particular, use System Dynamics to consider how and why the security control structure might change over time, potentially leading to ineffective controls.

5.2. Analysis of Pre-9/11 System

In "The Law of Loopholes in Action", David Gelernter argues that "every loophole will eventually be exploited; every loophole will eventually be closed" [35]. According to Fricker [19]:

> The effect of the Law of Loopholes, as anyone that flies regularly today knows, is an ever-expanding set of security measures and requirements put in place, generally in response to past security breaches. Such rules and requirements are useful for helping prevent a reoccurrence of a particular incident. But, to the extent a determined adversary's focus is on causing destruction and mayhem, these types of rules and requirements simply mean that as one loophole is plugged the adversary shifts its attention and energies to looking for and then trying to exploit a different loophole.

Instead of participating in the Law of Loopholes game, a STAMP-based analysis takes a top-down approach to proactively design and operate systems to meet security requirements and prevent the instantiation of system-level threats. Air transportation systems must control against the following threats:

1. A terrorist takes control of or disrupts an aircraft or persons onboard.
2. A terrorist takes control of or impersonates air traffic control.
3. A terrorist sabotages an aircraft.
4. A terrorist shoots an aircraft down.
5. A terrorist disrupts the critical infrastructure of the air transportation system (e.g. destroy a runway or radar).
6. A terrorist interferes with the aircraft communication, navigation, or surveillance systems.

However, before a threat assessment of the Next Generation Air Transportation System is conducted, the existing socio-technical control structure must be analyzed. It is useful to understand the lessons of 9/11 and keep them in mind in the evolution toward NGATS.

The reconstruction of a security incident begins with identifying the threat

carried out by the attacker as well as the constraints that were violated. After that, the taxonomy of inadequate controls is used to identify the dysfunctional interactions that enabled the violation of security constraints. In general, for each component in the control structure, the following items are provided [23]:

1. Constraints
2. Controls
3. Context
   a. Roles and Responsibilities
   b. Environmental and Behavior Shaping Factors
4. Flaws in the Controlled Process
5. Dysfunctional Interactions, Failures, Flawed Decisions, and Erroneous Control Actions
6. Reasons for Flawed Control Actions and Dysfunctional Interactions
   a. Control Algorithm Flaws
   b. Incorrect Process, Interface, or Mental Models
   c. Inadequate Coordination among Multiple Controllers
   d. Reference Channel Flaws
   e. Feedback Flaws

This model is a useful tool to understand how and why the security constraints were violated.

The security control structure for air transportation in the US in 2001 is shown below in **Figure 3**. The red, dotted lines indicate instances of inadequate communication and control.

To illustrate the technique, the Airport Security component on the above diagram is examined below:

Airport Security

In 2001, private companies were contracted to perform the passenger and baggage screening function at US Airports. Airports and carriers provided policies, resources, and instructions, but a clear line of accountability was not present to ensure that these directives were successfully executed.

Security Constraint Violated: Security personnel must remove passengers that are judged to be a risk to the air transportation system and contact law enforcement officials.

Controls: Computer Assisted Passenger Pre-Screening Systems (CAPPS), verification of ID, metal detectors, and X-Ray bag screening were the primary controls in place to enforce the constraint.

Context: The FBI and FAA were responsible for administering CAPPS. Those tagged by the system would then be subject to more rigorous baggage screening for explosives. CAPPS did not specify special screening of the passengers themselves.

Flaws in the Controlled Process: CAPPS, and the passenger screening system in general, did not have a specified mechanism to prevent high risk passengers from boarding an aircraft.

Dysfunctional Interactions, Failures, Flawed Decisions, and Erroneous

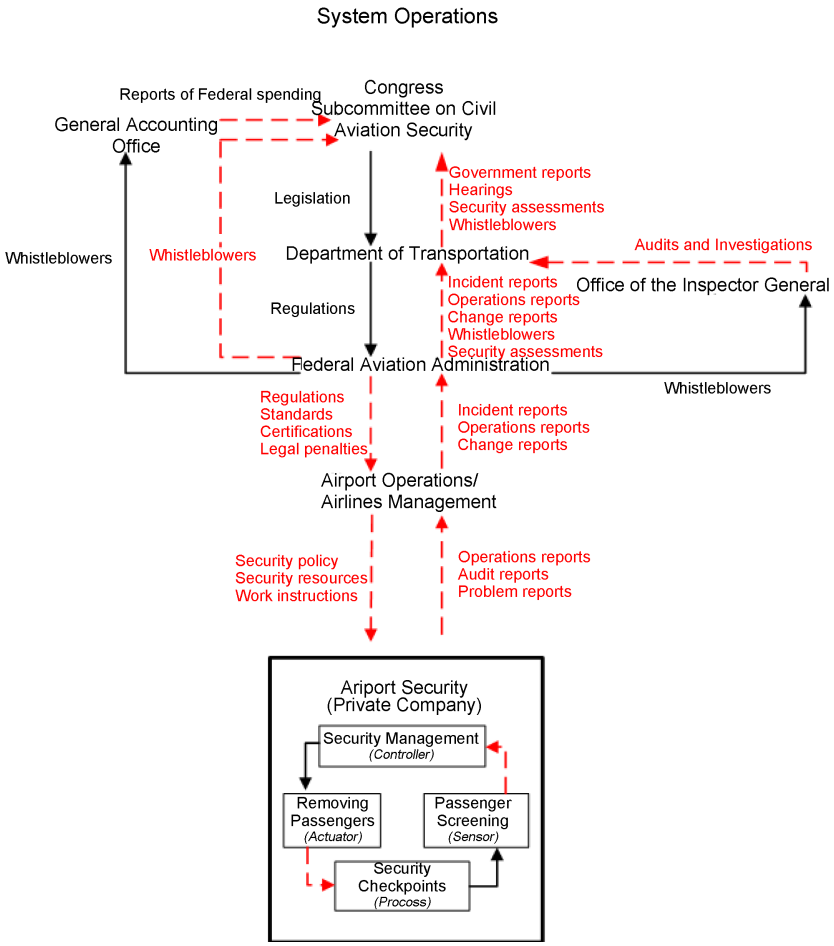

Figure 3. A high level control structure for pre-9/11 air transportation system.

Control Actions: At Logan International Airport, Wail al-Shehri and Satam al-Suqami were chosen for special screening of their checked bags, before they boarded American Airlines Flight 11. CAPPS identified Waleed al-Shehri but he did not check any luggage. Portland Airport identified Mohamed Atta. The hijackers of AA Flight 77, Hani Hanjour, Khalid al-Mihdhar, and Majed Moqed were also identified by CAPPS. Nawaf al-Hazmi and Salem al-Hazmi were chosen because of insufficient identification. United Airlines Flight 93's hijacker, Ahmad al-Haznawi, was flagged but none of the hijackers of United Airlines Flight 175 were identified by CAPPS [36].

Reasons for Flawed Control Actions and Dysfunctional Interactions: US airliners had not been hijacked in over a decade and a false sense of security was present. In the late 1990s, a Fox News/Opinion Dynamics poll indicated that 78% of Americans surveyed thought poor maintenance was "a greater threat to airlines safety" than terrorism. Also, increasing demand for flights led airliners to focus on changes to the system that improved throughput. The "Passenger Bill of Rights" emphasized providing a convenient and efficient passenger experience. According to statements from the 9/11 Commission, "Domestic hijacking in particular seemed like a thing of

the past". [36] Finally, screeners have a very monotonous job and are paid a low wage. These environmental conditions do not enable motivated, diligent execution of duties.

There are many ways that inadequate control can lead to a security system being compromised. STAMP provides a useful categorization scheme that captures most control flaws. Broadly, they fall into one of three categories: Inadequate enforcement of constraints, inadequate execution of control actions, or inappropriate or missing feedback [37]. The introduction of a malicious agent does not violate the assumption of the taxonomy originally developed for safety. In a safety scenario, poor engineering or management may offer inadequate enforcement of constraints, execution of control actions, or feedback such that a hazard that is "exploited" inadvertently in system operations. In a security scenario, poor engineering or management may offer inadequate enforcement of constraints, execution of control actions, or feedback such that a vulnerability is created that may be intentionally exploited in system operation. Whether one is concerned with safety or security, the problem is inadequate control. STAMP-Sec extends the safety list to capture security issues:

1. Inadequate Enforcement of Constraints (Control Actions)
   1.1. Unidentified threats
   1.2. Inappropriate, ineffective, or missing control actions for identified threats
      1.2.1. Design of control process does not enforce constraints
         1.2.1.1. Flaws in creation process
         1.2.1.2. Process changes without appropriate change in control (asynchronous evolution)
         1.2.1.3. Incorrect modification or adaptation
      1.2.2. Process models inconsistent, incomplete, or incorrect
         1.2.2.1. Flaws in creation process
         1.2.2.2. Flaws in updating process (asynchronous evolution)
         1.2.2.3. Time lags and measurement inaccuracies not accounted for
      1.2.3. Inadequate coordination among controllers and decision makers (boundary and overlap areas)
2. Inadequate Execution of Control Action
   2.1. Communication flaw
   2.2. Inadequate actuator operation
   2.3. Time lag
3. Inadequate or missing feedback
   3.1. Not provided in system/organizational design
   3.2. Communication flaw
   3.3. Time lag
   3.4. Inadequate detection mechanisms

The reader should take note that many of these inadequacies are not associated with simply an event-based risk. Rather, *flaws in communication and control* as well as *time lags* and *flaws in the design process* contribute to threats.

5.3. Analysis of Post-9/11 System

Now that the STAMP framework has been used to understand the attack of 9/11/2001, one can begin to study the air transportation system since then. Improvements have certainly been made over the last years. The creation of the Terrorism Threat Integration Center, a more vigilant civil defense program, an improved port and commercial shipping inspection program, hardened cockpits, and other changes have changed the security landscape. As a result, many attacks have been thwarted since 9/11 [22]. This is due to improvements in the security of the ATS as well as increased "human vigilance, unprecedented law enforcement, security, and intelligence cooperation, and the worldwide hunt for Al Qaeda, denying the group time, space, and resources to plan and mount spectacular attacks" [38].

However, this is certainly not the time for complacency to set in. Since 9/11, the State Department has warned that Al Qaeada (Sunni Islamists), Hizballah (Shia Islamists), Al Gama'a Al-Isalamiyya (Egyptian Islamists), Kahane Chai (Israeli extremists), Mujahdein e-Khalq (Marxist-Islamists) are believed to be operating in the US. Fortunately, many of the major flaws in the control processes and the dysfunctional interactions identified above have been corrected.

With regard to the Airport Security component example above, a number of changes have been made. The Department of Homeland Security (DHS) was established on November 25 by the Homeland Security Act of 2002. This decision introduced organizational complexity to the ATS because two executive departments share control of the ATS. The Transportation Security Administration (TSA) was created to replace the private companies that airlines contracted to perform passenger and baggage screening. As a part of DHS, the Administrator of the TSA is an Assistant Secretary of Homeland Security. With a cabinet level department focused on security, there is greater likelihood that poor red team results and whistleblowers will not be ignored. Additionally, the TSA imposes security policies, shares security resources, and informs work instructions for the airports and airlines. While the transformation of passenger screening from a private entity to the government does not necessarily improve security, it is preferable to have the screening organization reporting to the DHS rather than the airlines. DHS can impose the necessary control on TSA without being concerned about airline profitability.

The pressing question that arises in the context of developing NGATS is:

How can the JPDO evolve the current systems such that security does not degrade and perhaps even improves?

Dulac [39] has shown that the transition of a complex system from an operations environment to one that includes development introduces significant risks. Therefore, it is important that as the US transitions to the NGATS, the required communication and control from the earlier system is maintained and additional constraints are imposed to satisfy new security requirements. In order to achieve this objective, a high level model of socio-technical control is provided below in **Figure 4**.

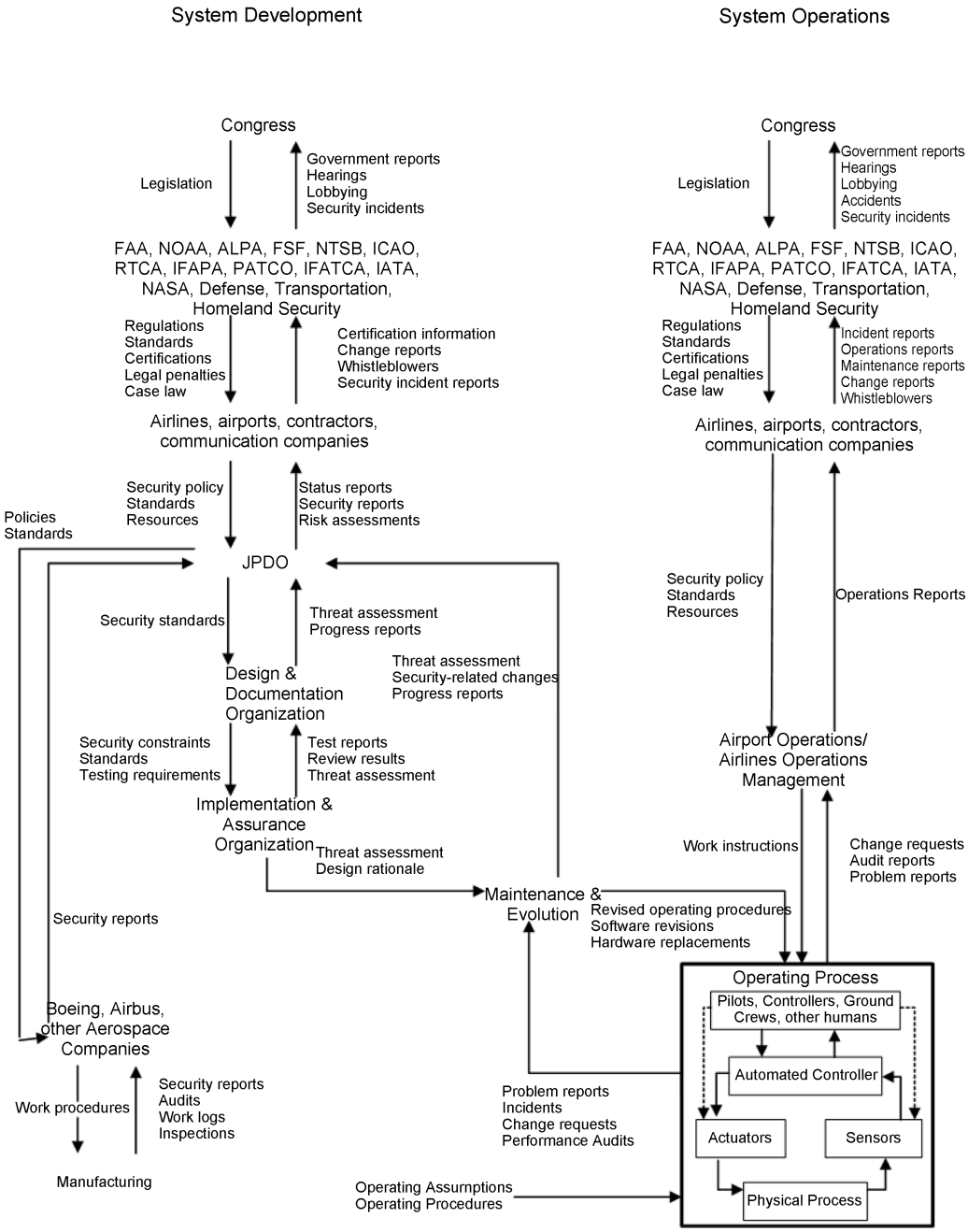

Figure 4. NGATS socio-technical control structure.

Risks emerge in a system when "basic inadequacies in the way individual components in the control structure fulfill their responsibilities" or when the "coordination of activities and decision-making can lead to unintended interactions and consequences" [40]. Therefore, the components in the control structure above should be analyzed to identify these risks. In general, a controller can provide four types of inadequate control [23]:

1. A required control action is not provided.
2. An incorrect control action is provided.
3. A potentially correct or adequate control action is provided too late (at the

wrong time).

4. A correct control action is stopped too soon.

The four inadequate controls are applied to the component responsibilities below to prevent poor engineering and management decision-making from enabling an attack.

To illustrate the technique, consider the level in the control structure that includes government regulatory agencies, industry associations, unions, courts, and other stakeholders which exert control over airports and airlines. They receive information from certification reports, incident reports, and whistleblowers. The Federal Aviation Administration (FAA), NOAA's Aviation Weather Service, Air Line Pilots' Association (ALPA), Flight Safety Foundation (FSF), National Transportation Safety Board (NTSB), International Civil Aviation Organization (ICAO), Radio Technical Commission for Aeronautics (RTCA), International Federation of Air Line Pilots Association (IFAPA), Professional Air Traffic Controller Organization (PATCO), International Federation of Air Traffic Controllers' Association (IFATCA), and International Air Transport Association (IATA) all influence the creation of standards, regulations, and certifications.

Figure 5 is a control structure diagram showing the lines of communication

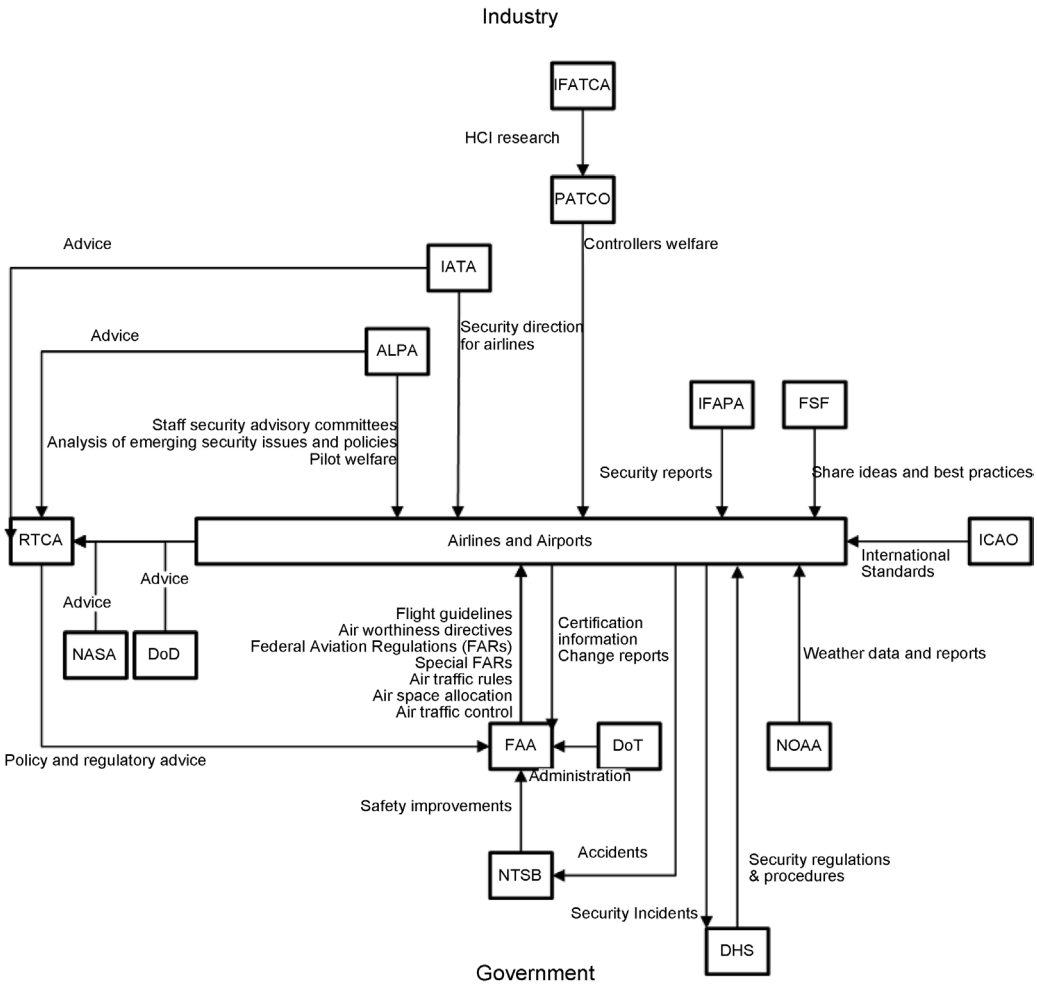

Figure 5. Current airline/airport control structure.

and control for the airlines and airports in the pre-NGATS environment. As the system evolves and NGATS is implemented, it is important that security-critical feedback is not lost. For example, the Radio Technical Commission for Aeronautics (RTCA) plays an important role by synthesizing the interests and advice of industry associations, unions, airlines, airports, and governmental entities, and developing policy and regulatory advice for the FAA to influence the airlines and airports. The alignment of stakeholders on security objectives is essential to success. Key responsibilities and risks for Executive Departments and Agencies are shown below in Table 2.

Once the organizational risks have been elucidated, it is appropriate to consider the security implications of two major changes to operation of the aircraft themselves: removal of human(s) and removal of voice communications as a standard communication medium. There is no question that the removal of humans eliminates an entire class of security vulnerabilities. Nevertheless, automation has not been shown to be inherently more secure. When done improperly, automation can inject vulnerabilities. Similarly, voice communications are often involved in security incidents. However, any PC user that has gotten a virus or been involved in a distributed denial of service (DDoS) attack knows that computer-to-computer digital communication is often not secure. Leveson explains the need for humans in automated systems in [41]:

> Computers and other automated devices are best at trivial, straightforward tasks. An *a priori* response must be determined for every situation: An algorithm provides predetermined rules and procedures to deal only with the set of conditions that have been foreseen. Not all conditions are foreseeable,

Table 2. Inadequate controls for executive agencies.

Item	Responsibility	Inadequate Control
	Executive Departments and Agencies	
1	Issue security regulations and procedures	DHS regulations and procedures have not identified important vulnerabilities or threats.
		DHS regulations and procedures create new vulnerabilities and threats.
		DHS regulations and procedures are only issued after an attack has occurred.
		DHS regulations and procedures are rescinded in response to external pressure.
2	Issue flight guidelines, aviation regulations, and air traffic rules	FAA does not receive necessary policy and regulatory advice from the RTCA and proper administration from the DoT.
		RTCA advice and DoT administration interferes with the FAA's ability to issue guidelines, regulations, and air traffic rules that promote strong security.
		RTCA advice and DoT administration are not provided to the FAA until after an attack has occurred.
		RTCA advice and DoT administration are not present during a critical period.
3	Provide leadership for the development and operation of NGATS	Senior leadership lacks competence or places minimal priority on security issues and therefore does not adequately implement the security strategy.
		Senior leadership intentionally disrupts the security strategy.
		Senior leadership does not exercise good judgment or place priority on security issues in the period before an attack.
		Senior leadership stops providing competent judgment and making security a priority due to external pressure.

> however, especially those that arise from a combination of events, and even those that can be predicted are programmed by error-prone humans… Human operators are included in complex systems because, unlike computers, they are adaptable and flexible… Humans can exercise judgment and are unsurpassed in recognizing patterns, making associative leaps, and operating in ill-structured, ambiguous situations.

Pilots, air traffic controllers, radio operators, and others involved in the operation of aircraft must be aware of four classes of inadequate control actions that could interfere with their primary responsibility of operating the system without security incidents. For example (see **Table 3**)

Midkiff *et al.* [42] offer a detailed overview of aircraft operation procedures. Historically, these procedures have not been exploited to accomplish terrorist objectives. The reason for this is that attackers will almost always pursue the vulnerability that is most easily exploited. In this case, the vulnerabilities associated with passenger and cargo screening were blatantly obvious and enabled (suicide) hijackers to board an aircraft and take control. The current control structure for aircraft operations is shown below. The essential communication and control between aircraft, ground assets, and satellites are highlighted. As a representative example, threat six:

A terrorist interferes with the aircraft communication, navigation, or surveillance systems

will be analyzed. see **Figure 6**.

During a flight, the airline communicates with an aircraft over a VHF radio. In the event of an emergency, if the aircraft is out of communication range with the airline, the cockpit may attempt to communicate with other aircraft or ground assets over the emergency channel. The second VHF radio is used to communicate with other aircraft in flight or air traffic control. Weather and traffic data is passed along over this channel. Finally, a HF radio is also required to provide over-water communications with ATC.

A variety of digital data links also exist to send data between aircraft and ground assets. The Aircraft Communication Addressing and Reporting System (ACARS) enables aircraft to transmit location (from GPS), altitude, and velocity information stored in the Flight Management System procedures (FMS) computer to ATC over a satellite link. Similarly, ATC can send messages back to the

Table 3. ATS operator security.

Responsibility	Inadequate Control
Aircraft and Ground Operators	
Operate the system without security incidents	ATS Operators make bad decisions because of poor assumptions and procedures.
	ATS Operators choose to make decisions contrary to security objectives.
	ATS Operators does not make security decisions in a timely manner.
	ATS Operators make decisions supporting security but do not follow through and therefore have insufficient impact.

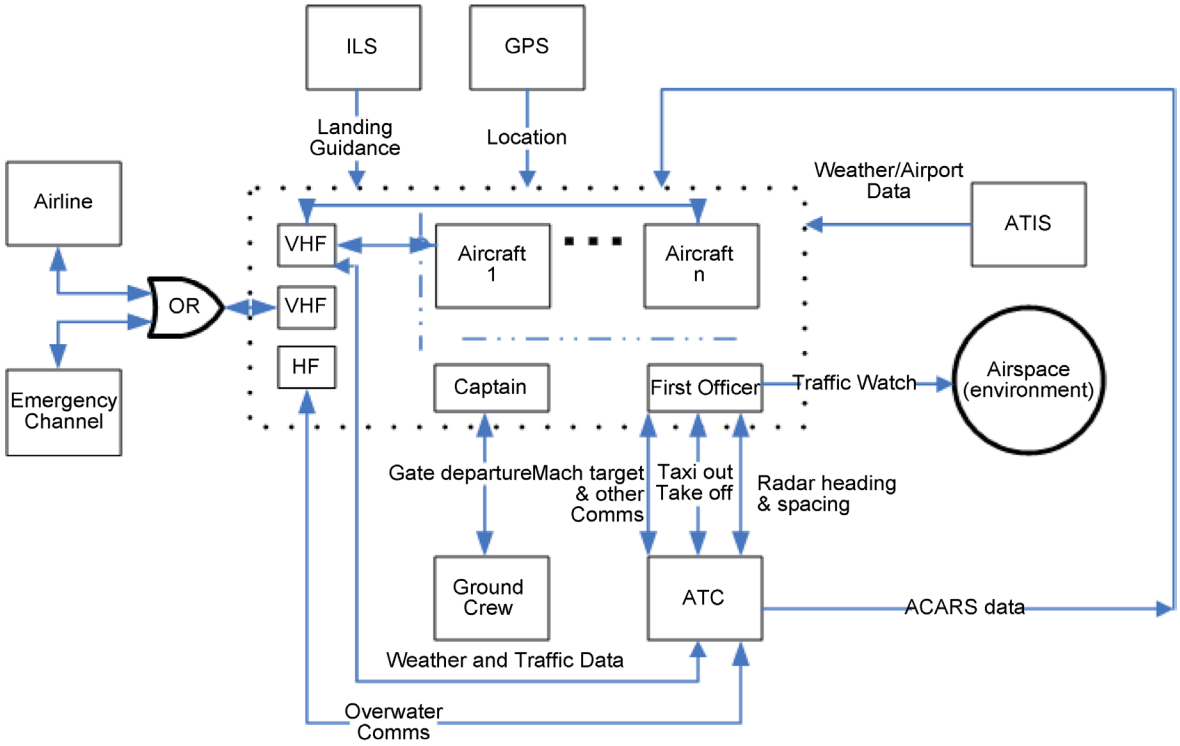

Figure 6. Current aircraft/ATC control structure.

FMS. Vital communications during the final phases of flight include position data from the Instrument Landing Systems (ILS) and automated audio recordings of non-control airport data (e.g. weather conditions) from the Automatic Terminal Information Service (ATIS).

Not surprisingly, the captain and first officer also play a key role in the control structure. Prior to takeoff, the captain coordinates activities with the ground crew while the first officer receives taxi out and take off information from ATC. Once the aircraft is airborne, the captain controls the aircraft as the first officer provides visual traffic watch, inputs the radar heading and spacing, sets the mach target, and handles any other additional communications with ATC.

With the drastic changes made to the ATS socio-technical control structure following 9/11, terrorists will likely be more inclined to instantiate threats in the operation of aircraft procedures. Many of the changes in the control structure for NGATS are captured in Figure 7 below.

Immediately, one notices the fact that the traffic watch and early phase communications fall to the Captain. Additionally, a data network will be incorporated and used in place of voice communications (although voice communication equipment will still be onboard). The security requirements, control actions, and potential inadequate controls for the three principal components in this control structure are provided next.

Cockpit Crew (Captain and First Officer)

Security Constraints:

1. It must not be possible to disable TCAS from the cockpit. TCAS shall be functioning before ATC authorizes takeoff.

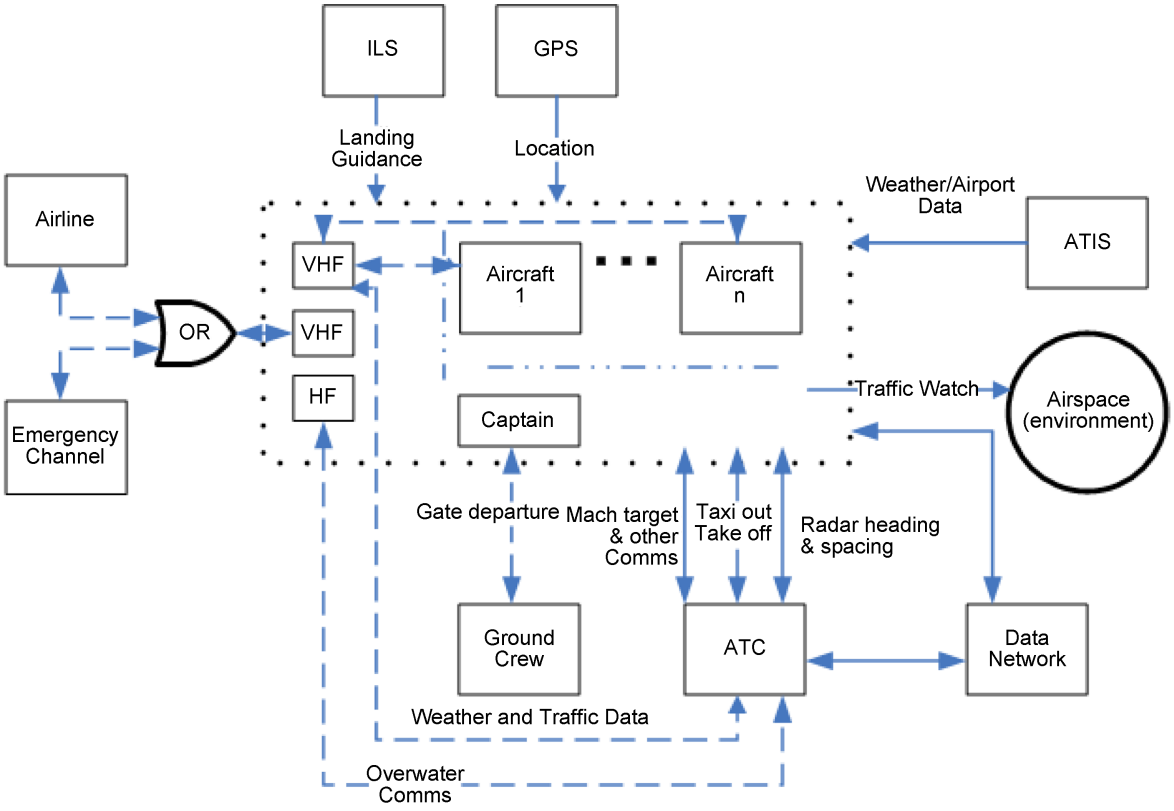

Figure 7. Possible NGATS aircraft/ATC control structure.

2. Pilots shall make setting the appropriate velocity a top priority.
3. Pilots shall make resetting the altimeter a top priority.
4. Pilots shall confirm over secure voice communications any suspicious ACARS data.
5. Cockpits shall display ATIS data visually as well as audibly.
6. Cockpits without crews (*i.e.* UAVs) shall have preprogrammed runways and landing information to be executed if communication with ATC is lost during descent, terminal area arrival, final approach, or landing.

Control Actions:

1. Regulation—Design: All new aircraft shall be designed to satisfy this security requirement. If the collision avoidance system is disabled, it is much easier for a terrorist to orchestrate a collision.
2. Regulation—Training and Standard Procedures: Operating procedures, flight simulators, and mandatory training shall equip pilots to set the appropriate velocity despite interruptions and distractions at different times. If the correct velocity is not set, it is much easier for a terrorist to orchestrate a collision.
3. Regulation—Training and Standard Procedures: Operating procedures, flight simulators, and mandatory training shall equip pilots to reset the altimeter despite interruptions and distractions at different times. If the correct altitude is not set, it is much easier for a terrorist to orchestrate a collision.
4. Regulation—Training and Standard Procedures: Operating procedures, flight simulators, and mandatory training shall equip pilots to verify suspicious

ACARS data over voice communications.

5. Regulation—Design: Human factors experts will be responsible for ATIS subsystem design. If a terrorist distracts a pilot in the later phases of flight and he misses important ATIS information, a text-based version of the report will allow him to quickly get the necessary data.
6. Regulation—Design: All UAVs certified for operations in the NGATS shall be designed to satisfy the preprogrammed runway requirement. In the event that communication between ATC and a UAV is jammed, the UAV must still successfully land. One way to do this is to preprogram before takeoff an assigned runway as well as other details necessary for the UAV to reach its destination airport if communication is lost.

Potential Inadequate Controls:

1. TCAS

a. Design regulations do not prohibit TCAS deactivation in the cockpit.

b. Design regulations require TCAS deactivation in the cockpit.

c. Design regulations prohibiting TCAS deactivation go into effect after NGATS certified aircraft are built.

d. Design regulations prohibiting TCAS deactivation are suspended during NGATS operations.

2. Setting Velocity

a. Procedures and training are insufficient to direct pilots to ensure that the correct velocity is set after they are interrupted.

b. Procedures and training form pilots that are careless about setting the target velocity.

c. Good procedures and training for setting the velocity target are developed too late.

d. Procedures and training for setting the velocity target are withdrawn.

3. Resetting Altimeter

a. Procedures and training are insufficient to direct pilots to ensure that the altimeter is reset at the proper time after they are interrupted.

b. Procedures and training form pilots that are careless about resetting the altimeter.

c. Good procedures and training for resetting the altimeter are developed too late.

d. Procedures and training for resetting the altimeter are withdrawn.

4. ACARS Data

a. Procedures and training are insufficient to direct pilots to ensure that suspicious ACARS data is verified with voice communications.

b. Procedures and training form pilots that do not verify suspicious ACARS data over voice communications.

c. Good procedures and training for verifying suspicious ACARS data over voice communications are developed too late.

d. Procedures and training for verifying suspicious ACARS data are withdrawn.

5. ATIS Subsystem

a. Design specifications do not require visual presentation of ATIS information.

b. Design specifications do not allow visual presentation of ATIS information.

c. Design specifications that mandate visual and audible presentation of ATIS information are created too late.

d. Design specifications that mandate visual and audible presentation of ATIS information are withdrawn.

6. UAVs

a. Design specifications do not require preprogrammed landing routines.

b. Design specifications do not allow preprogrammed landing routines.

c. Design specifications that mandate preprogrammed landing routines are created too late.

d. Design specifications that mandate preprogrammed landing routines are withdrawn.

The final step of a STAMP-based analysis is System Dynamics (SD) modeling. System Dynamics is used to understand how the static control structure designed in the earlier stages *and* the attackers themselves could evolve. In particular, one is interested in evolution to insecure states such that security constraints would no longer be enforced by components in the socio-technical system. Unlike system safety engineering in which many risks and hazards are "generated" endogenously within the socio-technical system, security engineering risks and threats often develop exogenously. While the "insider-threat" must be addressed, malicious actors outside of the ATS must be modeled. Terrorist groups such as Al Qaeda, are an example of an exogenous factor. To illustrate the SD modeling approach, a causal loop diagram model of terrorism and the outside factors that influence it was developed and analyzed.

System Dynamics theoretical basis comes from control systems and non-linear dynamics. Complex systems, whether they are technical, organizational, or some combination, often exhibit highly non-linear behavior where the relationship between cause and effect is not intuitively obvious. According to Martinez-Moyano *et al.* [43]:

> System Dynamics is a computer-aided approach to policy analysis and design that applies to dynamic problems arising in complex social, managerial, economic, or ecological systems. Dynamic systems are characterized by interdependence, mutual interaction, information feedback, and circular causality.

System Dynamics models are constructed by a combination or positive (reinforcing) and negative (balancing) feedback loops in addition to state and rate variables [28].

At its lowest level, a SD model is a system of coupled, first order, non-linear ordinary differential equations presented in an easy to understand graphical form accessible to policy makers. The models can be simulated to obtain numerical results. In order to show the connection between traditional mathematics and SD visualizations, the figure below presents the graphical representation

of a differential equation. While this level of understanding is not necessary for policy makers and managers to benefit from causal loop diagrams, the diagram is shown to assist scientists and engineers learning System Dynamics. The state variable, *X*, is controlled by two rate variables, *Y* and *Z*. Three auxiliary variables also are also provided, *A*, *B*, and *T*, that define *Y* and *Z* and each other. This SD model integrates the differential equation shown over the state variable, *X*. See Figure 8 below.

The following quote by John Sterman, a leading scholar in the field, communicates the philosophy of System Dynamics [44]:

> While it's hard to define what system dynamics is, I don't have any trouble answering why it is valuable. As the world changes ever faster, thoughtful leaders increasingly recognize that we are not only failing to solve the persistent problems we face, but are in fact causing them. All too often, well-intentioned efforts to solve pressing problems create unanticipated "side effects". Our decisions provoke reactions we did not foresee. Today's solutions become tomorrow's problems. The result is policy resistance, the tendency for interventions to be defeated by the response of the system to the intervention itself. From California's failed electricity reforms, to road building programs that create suburban sprawl and actually increase traffic congestion, to pathogens that evolve resistance to antibiotics, our best efforts to solve problems often make them worse. At the root of this phenomenon lies the narrow, event-oriented, reductionist worldview most people live by. We have been trained to see the world as a series of events, to view our situation as the result of forces outside ourselves, forces largely unpredictable and uncontrollable… System dynamics helps us expand the boundaries of our mental models so that we become aware of and take responsibility for the feedbacks created by our decisions.

The "well-intentioned efforts to solve pressing problems create unanticipated 'side effects'" mentioned above will be explored in this paper's terrorism model.

Initially, in a model building activity, simple causal loop diagrams are developed that elucidate the non-linear cause-effect relationship. These qualitative models suggest policies that acknowledge feedback in the system and can prevent delayed unintended consequences. Causal loop diagrams, and more generally system archetypes [27] anchor the development of high fidelity, quantitative

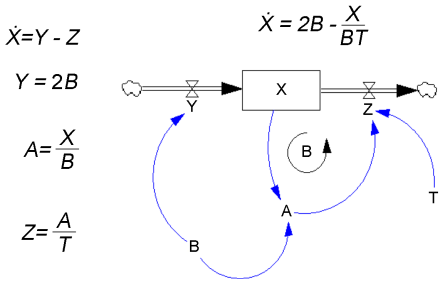

Figure 8. A differential equation implemented as a system dynamics model.

models that allow the use of simulation to explore scenarios and rigorously investigate dynamic hypotheses [45]. The causal loop diagram below (**Figure 9**) corresponds to Level 1 in the Owens-Dulac hierarchy [32]. It was developed by the author in a modeling activity with John Sterman and Kim Thompson.

The model contains the major feedback loops that govern the behavior of terrorists, such as those that would attack the ATS. In order to accomplish the goal of minimizing the Attractiveness of Terrorism, one must examine the reinforcing and balancing loops that influence terrorist behavior.

Retaliation Works (Balancing Loop)

The first balancing loop is called *Retaliation Works*. In this loop, one sees that as the *Attractiveness of Terrorism* increases, *Terrorist Attacks* increase, *Fear in Target Nation* increases, and so does *Retaliation*. The net effect of this is that *Attractiveness of Terrorism* decreases. This result was certainly not intended by the terrorists involved, but nonetheless has shown to be true in some instances (e.g. Barbary Pirates in 1815 and the Taliban Government in 2001).

Greater Isolation (Reinforcing Loop)

However, an increase in retaliation also has the potential to reinforce the *Attractiveness of Terrorism*. Retaliation has the effect of reducing the *Conventional Military and Political Power of Terrorist States*, thereby increasing the attractiveness of asymmetric warfare, such as the attack on 9/11. Part of this causal loop also has the potential, with a delay, to increase the *Ideological Acceptability of Terrorism*, thus increasing the *Attractiveness of Terrorism*.

Sanctions Work (Balancing Loop)

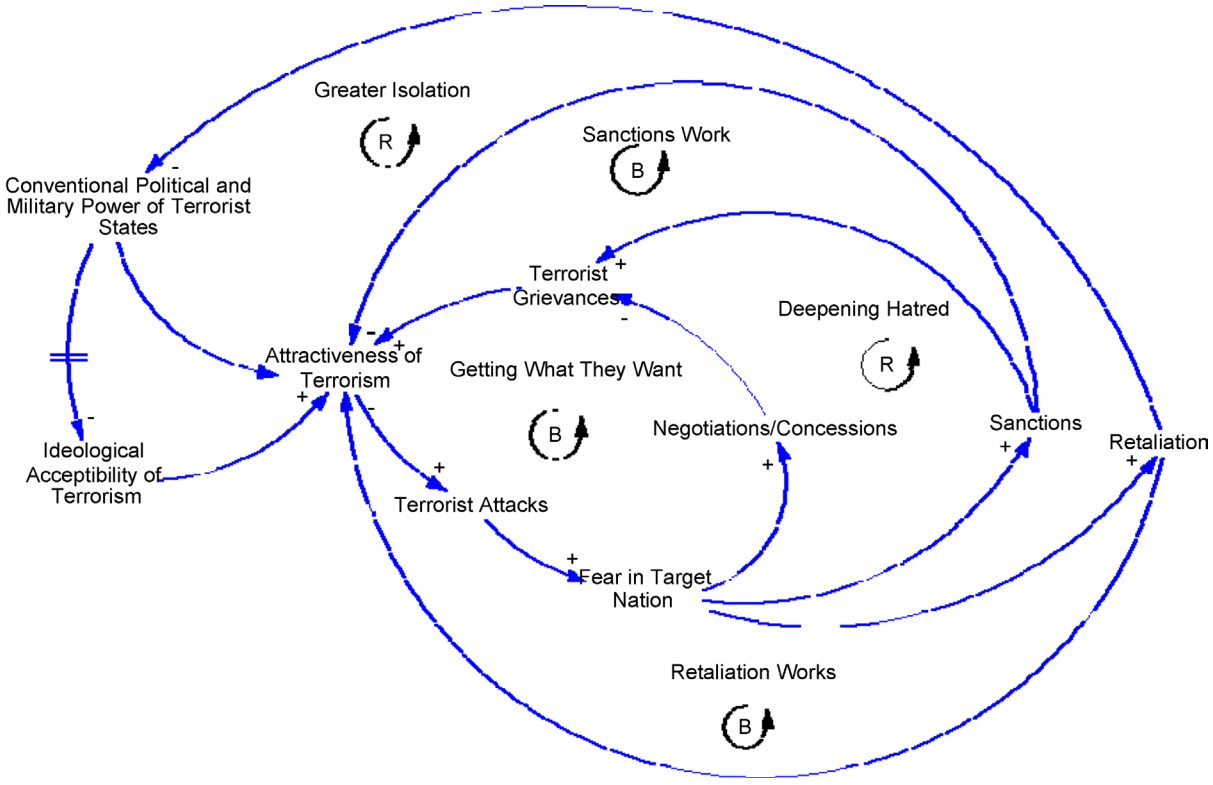

Figure 9. Causal loop diagram of terrorism.

Instead of retaliation, *Sanctions* are another option to be explored to mitigate the threat of terrorism. An increase in the *Attractiveness of Terrorism* will lead to an increase in the *Fear in Target Nation*, an increase in *Sanctions*, and finally a decrease in the *Attractiveness of Terrorism*.

Deepening Hatred (Reinforcing Loop)

However, *Sanctions* can also lead to deepening hatred. *Sanctions* may fuel *Terrorist Grievances* and therefore increase the *Attractiveness of Terrorism*. In the latter half of the twentieth century, economic sanctions against Middle Eastern states that support terror have been a cause for terrorists to incite populations against the United States.

Getting What They Want (Balancing Loop)

Another loop can create the situation where the increase in *Terrorist Attacks* leads to an increase in *Fear in Target Nation* that leads to an increase in *Negotiations/Concessions*. *Negotiations/Concessions* reduce *Terrorist Grievances* and finally reduce the *Attractiveness of Terrorism*. The terrorist attack in Spain on March 11, 2004 days before the national election led to the selection of a government sympathetic to the causes of Jihadists and the cessation of terrorist attacks in that country.

New strategies must be developed to prevent an attack as well as manage the aftermath. Informal, ad hoc approaches will almost certainly fall short of accomplishing the desired goal of little to no casualties [5]. A rigorous, systematic method is necessary to develop an appropriate approach. Traditional mathematical modeling has made significant contributions to this end. However, according to John Sterman, "The greatest potential for improvement comes when the modeling process changes deeply held mental models". [28] The author proposes an approach that brings the power of control theory in an accessible way to security professionals and policy makers involved in the US ATS. In consultation with air transportation security experts, future work in this area would involve defining the references modes for the key variables described above and instantiating a simulation model.

6. Conclusions

STAMP-Sec addresses many of the pitfalls associated with applying quantitative risk assessment and game theory to security problems. Additionally, it implicitly supports the use of red teaming to test that the socio-technical system has not evolved in such a way that security constraints are no longer enforced.

Unlike probabilistic risk assessment approaches [11], STAMP-Sec appropriately addresses the role of software, human factors, security culture, and design errors in the development of engineering systems. In fact, it explicitly addresses how to incorporate these key factors into the security requirements (*i.e.* constraints) of the ATS. The inherent flaws in the use of subjective probability (*i.e.* expert guessing) identified by Tversky and Kahneman [18] are completely avoided. No assumptions are made as to the adherence of system users and attackers to the axioms of rationality [46]. Perhaps most importantly, the engage-

ment between the attacker and the defender of the system has not been excessively simplified (e.g. abstracting the engagement to a two-stage Markov process) to facilitate modeling. Finally, the intelligence of the adversary is appreciated unlike reliability-based approaches that apply the 80/20 rule [14].

Similarly, the STAMP approach does not share the inherent weaknesses of game-theoretic security modeling. Game theory models of security often make simplifying assumptions, e.g. the attacker can only execute one attack at a time. STAMP-Sec does not engage in these types of assumptions. The fact that defenders and attackers may value targets differently is not relevant and no inappropriate mathematical assumptions are made such as the fact that the probability of an attack is a convex function of the defensive resource spending. If a STAMP-based executable simulation is developed, sensitivity analysis of System Dynamics models mitigates the uncertainty that initially exists with quantitative model parameters. Lastly, unlike game theory's emphasis on strategy, STAMP-Sec informs both the design and tactical operation of complex engineering systems.

STAMP-Sec provides concrete information that can be directly incorporated into requirements and design documents. Furthermore, it provides recommendations for how to address these security issues through the definition of constraints, responsible components, and control actions. Finally, the possible inadequate controls and causes for constraint violation are explored. Informational, operational, and physical security issues are addressed holistically. Notably, many of the security issues identified in this paper are not associated with the failure of any device or subsystem. Rather, threats emerge from inadequate control. By showing where communication and feedback could be lost in the transition from the current ATS to NGATS, many risks are identified. Additionally, given the use of increased automation in NGATS, STAMP-Sec is particularly applicable because it acknowledges the role that software plays in security incidents. In conclusion, the aforementioned strengths, sustained by the valuable results obtained for the Next Generation Air Transportation System, support the hypothesis that STAMP-Sec provides insight into security problems and motivates future research to further categorize its strengths and weaknesses.

References

[1] Anderson, R. (2001) Security Engineering. Wiley Computer Publishing, New York.

[2] JPDO (2004) Next Generation Air Transportation System Integrated Plan. Joint Planning and Development Office.

[3] Krenzke, T. (2006) Ant Colony Optimization for Agile Motion Planning. MIT, Cambridge.

[4] Barlas, S. (1996) Anatomy of a Runaway: What Grounded the AAS. *IEEE Software*, **13**, 104-106. https://doi.org/10.1109/MS.1996.476294

[5] Laracy, J. (2006) A Systems Theoretic Accident Model Applied to Biodefense. *Defense and Security Analysis*, **22**, 301-310. https://doi.org/10.1080/14751790600933905

[6] Apostolakis, G. (2000) The Nuclear News Interview—Apostolakis: On PRA. *Nuclear News*, 27-31.

[7] Laracy, J. (2007) Addressing System Boundary Issues in Complex Socio-Technical Systems. *Proceedings of the 5th Annual Conference on Systems Engineering Research*, Hoboken, NJ.

[8] Feynman, R.P. (1986) Rogers Commission Report: Appendix F—Personal Observations on the Reliability of the Shuttle. NASA.

[9] Stamatelatos, M.G. (2002) New Thrust for PRA at NASA.

[10] Scottberg, E. (2006) NASA Says Shuttle Risk Overstated; Yet Some Risk Unavoidable. *Popular Mechanics*, 30 June 2006.

[11] Apostolakis, G.E. (2004) How Useful Is Quantitative Risk Assessment? *Risk Analysis*, **24**, 515-520. https://doi.org/10.1111/j.0272-4332.2004.00455.x

[12] Parker, D.B. (2007) Risks of Risk-Based Security. *Communications of the ACM*, **50**, 120. https://doi.org/10.1145/1226736.1226774

[13] Laracy, J.R. (2007) A System-Theoretic Security Model for Large Scale, Complex Systems Applied to the Next Generation Air Transportation System (NGATS). Master of Science Thesis, MIT, Cambridge.

[14] Bier, V.M. (2005) Game-Theoretic and Reliability Methods in Counter-Terrorism and Security Modern Statistical and Mathematical Methods in Reliability: Series on Quality, Reliability and Engineering Statistics. World Scientific Publishing Co., Singapore.

[15] Frey, B.S. and Luechinger, S. (2003) How to Fight Terrorism: Alternatives to Deterrence. *Defense and Peace Economics*, **14**, 237-249. https://doi.org/10.1080/1024269032000052923

[16] Sandler, T., Daniel, G. and Arce, M. (2003) Terrorism and Game Theory. *Simulation and Gaming*, **34**, 317-337. https://doi.org/10.1177/1046878103255492

[17] Banks, D.L. and Anderson, S. (2007) Combining Game Theory and Risk Analysis in Counterterrorism: A Smallpox Example. In: Wilson, A.G., Wilson, G.D. and Olwell, D.H., Eds., *Statistical Methods in Counterterrorism*: *Game Theory*, *Modeling*, *Syndromic Surveillance*, *and Biometric Authentication*, Springer, New York.

[18] Tversky, A. and Kahneman, D. (1974) Judgment under Uncertainty: Heuristics and Biases. *Science*, **185**, 1124-1131. https://doi.org/10.1126/science.185.4157.1124

[19] Fricker, R.D. (2005) Game Theory in an Age of Terrorism: How Can Statisticians Contribute? In: Wilson, A.G., Wilson, G.D. and Olwell, D.H., Eds., *Statistical Methods in Counterterrorism*: *Game Theory*, *Modeling*, *Syndromic Surveillance*, *and Biometric Authentication*, Springer, Berlin.

[20] Schneider, W. (2003) The Role and Status of DoD Red Teaming Activities. *Paper presented at the Defense Science Board*, September 2003.

[21] Dzakovic, B. (2003) Statement of Bogdan Dzakovic to the National Commission on Terrorist Attacks upon the United States.

[22] NCTAUS (2004) 9/11 Commission Report. *Paper presented at the National Commission on Terrorist Attacks upon the United States*.

[23] Leveson, N. (2002) System Safety Engineering: Back to the Future. Cambridge.

[24] Graham, S., Baliga, G. and Kumar, P.R. (2004) Issues in the Convergence of Control with Communication and Computing: Proliferation, Architecture, Design, Services, and Middleware. 43*rd IEEE Conference on Decision and Control*, **2**, 1466-1471.

[25] Checkland, P. (1981) Systems Thinking, Systems Practice. John Wiley & Sons, New York.

[26] Ashby, W.R. (1956) An Introduction to Cybernetics. Chapman and Hall, London.

[27] Senge, P. (2006) The Fifth Discipline. Double Day, New York.

[28] Sterman, J. (2000) Business Dynamics: Systems Thinking and Modeling for a Complex World. Irwin McGraw-Hill, Boston.

[29] Kirby, M.W. (2003) The Intellectual Journey of Russell Ackoff: From OR Apostle to OR Apostate. *Journal of the Operational Research Society*, **54**, 1127-1140. https://doi.org/10.1057/palgrave.jors.2601627

[30] Richmond, B. (1993) Systems Thinking: Critical Thinking Skills for the 1990s and Beyond. *System Dynamics Review*, **9**, 113-133. https://doi.org/10.1002/sdr.4260090203

[31] Gharajedaghi, J. (1999) Systems Thinking: Managing Chaos and Complexity. Butterworth Heinemann, Boston.

[32] Dulac, N., *et al.* (2007) Demonstration of a Powerful New Dynamic Approach to Risk Analysis for NASA's Constellation Program. MIT Complex Systems Research Laboratory Report, Cambridge.

[33] Rae, A., Fidge, C. and Wildman, L. (2006) Fault Evaluation for Security-Critical Communications Devices. *Computer*, **39**, 61-68. https://doi.org/10.1109/mc.2006.161

[34] Leveson, N. (2003) A New Approach to Hazard Analysis for Complex Systems. *Paper presented at the International Conference of the System Safety Society*, Ottawa.

[35] Gelernter, D. (2005) The Law of Loopholes in Action. *Los Angeles Times*, 6 May 2005.

[36] NCTAUS (2004) The Aviation Security System and the 9/11 Attacks—Staff Statement No. 3. *Paper presented at the National Commission on Terrorist Attacks Upon the United States*.

[37] Leveson, N. (2004) A New Accident Model for Engineering Safer Systems. *Safety Science*, **42**, 237-270.

[38] RMS (2003) Managing Terrorism Risk. Risk Management Solutions, Inc.

[39] Dulac, N. (2007) A Framework for Dynamic Safety and Risk Management Modeling in Complex Engineering Systems. Ph.D. Thesis, MIT, Cambridge.

[40] Leveson, N., Dulac, N., Barrett, B., Carroll, J., Cutcher-Gershenfeld, J. and Friedenthal, S. (2005) Risk Analysis of NASA Independent Technical Authority. MIT, Cambridge.

[41] Leveson, N.G. (1995) Safeware. Addison-Wesley Publishing Co., Reading.

[42] Midkiff, A.H., Hansman, R. and Reynolds, T. (2004) Air Carrier Flight Operations. ICAT Report, MIT, Cambridge.

[43] Martinez-Moyano, I.J., Rich, E., Conrad, S., Anderson, D.F. and Stewart,T.R. (2005) A Behavioral Theory of Insider-Threat Risks: A System Dynamics Approach. Retrieved from Albany, NY.

[44] Sterman, J. (2002) All Models Are Wrong: Reflections on Becoming a Systems Scientist. *System Dynamics Review*, **18**, 501-531. https://doi.org/10.1002/sdr.261

[45] Gonzalez, J.J., *et al.* (2005) Helping Prevent Information Security Risks in the Transition to Integrated Operations. *Telektronikk*, **101**, 29-37.

[46] Savage, L.J. (1954) The Foundations of Statistics. Wiley, New York.